INDUSTRIAL COMMUNICATION JOURNAL

ETHERNET WIRELESS SECURITY

Cyberrisiken in digitalen Ökosystemen

Systemischer Schutz

Seite 44

genua.

Bild: genua gmbH

Cyberrisiken in digitalen Ökosystemen

Systemischer Schutz

Einer der fundamentalsten Trends in der Industrie sind digitale Ökosysteme. Lieferbeziehungen und Wertschöpfung funktionieren damit nicht mehr linear, sondern mehrdimensional und vernetzt. So große Chancen digitale Ökosysteme auch bieten: Sie erhöhen gleichzeitig die Anfälligkeit für Cyberangriffe. Um sie sicher und zuverlässig zu nutzen, bedarf es daher ausgefeilter, mehrstufiger Schutzmechanismen.

In der Vergangenheit waren Lieferketten mehr oder minder eindimensional – Rohstoffe und Vorprodukte wanderten Stufe um Stufe die Lieferkette entlang, bis das Endprodukt den Kunden erreichte. Dem Weg der physischen Produkte folgten mit zunehmender Digitalisierung allmählich auch Daten, jedoch oft genug ausgebremst durch Medienbrüche, inkompatible Systeme und proprietäre Datenformate. Das änderte sich mit der Industrie 4.0. Um die Chancen der Digitalisierung effektiver zu nutzen, wurden verstärkt Datenformate, Kommunikationsprotokolle und Schnittstellen standardisiert. MQTT und OPC UA, RAMI 4.0 und digitaler Zwilling (Verwaltungsschale) sind nur einige Bausteine dieser Entwicklung. Auf dieser Grundlage konnten sich digitale Ökosysteme auch in der Industrie etablieren. Lieferbeziehungen sind in zunehmendem Maße nicht mehr linear, sondern mehrdimensional. Über zentrale Plattformen mit standardisierten Schnittstellen können sich Unternehmen mit ihren Leistungen schnell und einfach einklinken, sei es z.B. als Zulieferer von Stoffen und Waren, als Dienstleister für die Produktveredelung, als Service-Anbieter, der zusätzliche Maschinenfunktionen etabliert oder datenbasiert Anlagen optimiert. IIoT-Plattformen, digitale Marktplätze, Börsen für modulare Software-Erweiterungen und Smart Services sind nur einige Beispiele für diese Entwicklung. Was diese digitalen Ökosysteme in der Industrie kennzeichnet: Die Akteure leiten nicht einfach die Daten in digitaler Form weiter. Sie haben Zugriff auf Systeme und Applikationen, dienen diesen als externe Datenquelle und zur Datenverarbeitung oder sogar als Teil der Steuerung von Anlagen. Digitale Ökosysteme leben von Offenheit, Anpassungsfähigkeit und Vernetzung. Menschen, Maschinen, Prozesse sowie IT, OT, IIoT und Cloud-Infrastrukturen werden über unterschiedliche Schnittstellen und integrierte Prozesse verbunden.

Smart, open, viable – und verletzlich

Was zunächst mit einer Automatisierung von Prozessen begann, geht inzwischen immer häufiger in eine (Teil-)Autonomie von Sys-

Bilder der Doppelseite: genua gmbH

temen über. Diese wirkt auf intelligente und effiziente Weise zusammen und ermöglicht neue Szenarien in Logistik, Konstruktion, Produktion und Vertrieb. Das bedeutet auch: autonomen Zugang von einem System zum nächsten. Digitale Ökosysteme ermöglichen neue Geschäftsmodelle as-a-Service, bieten Wachstums- und Effizienzhebel, steigern die Flexibilität, vereinfachen Monitoring und Wartung von einzelnen Maschinen bis hin zu ganzen Anlagen per Remote-Services und erlauben eine zum Teil sprunghafte Verbesserung der Gesamtanlageneffektivität (Overall Equipment Effectiveness, OEE). Doch die neue Offenheit und starke Vernetzung führen zu einer wachsenden Vulnerabilität gegenüber Cyberangriffen auf die Verfügbarkeit generell sowie die Funktion der einzelnen Systeme, sowohl durch bekannte Cyberrisiken als auch neue Angriffsszenarien. Ein spezieller Schwachpunkt ist die Integration alter Maschinen (Retrofitting), die nicht unter den Gesichtspunkten der Digitalisierung und Cyber-Security designt wurden. Und auch das vermeintliche Einschränken des Netzwerkzugangs auf ausgewählte Partner im digitalen Ökosystem reicht nicht aus, wenn diese wiederum angreifbar sind.

Vier häufige Schwachpunkte

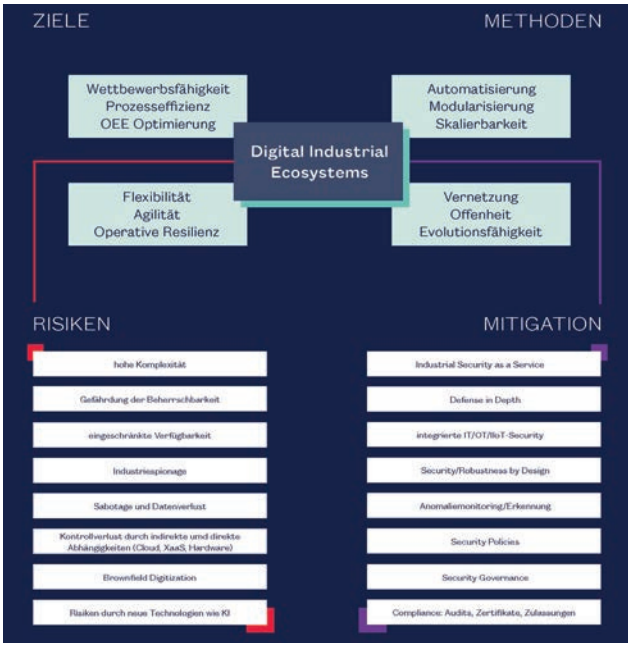
Genua, ein Anbieter von IT-Sicherheitslösungen für digitale Infrastrukturen, hat die Gefährdungen innerhalb industrieller digitaler Ökosysteme als vier zentrale Risiken formuliert:

- Abnehmende Beherrschbarkeit der eigenen Infrastrukturen durch hohe Komplexität und Vielfalt des Gesamtsystems.
- Steigende Angriffsfläche durch unsichere digitale Integration älterer Anlagen und Maschinen (Brownfield Digitization).
- Einschränkung der Verfügbarkeit sowohl durch Datenverluste und Sabotage gegen die Unternehmen selbst als auch durch Angriffe auf Dienstleister und Lieferanten.
- Zunehmend komplexe und fragile Abhängigkeiten von Geschäftspartnern durch digitale Supply Chains, Einsatz von Fremdsystemen (Hard- und Software) sowie Fremddiensten in eigenen Netzen und in der Cloud.

Um diesen Herausforderungen wirkungsvoll zu begegnen, muss Cyber-Security strategisch, technologisch und organisatorisch verankert werden. Das bedeutet, zahlreiche Maßnahmen auf verschiedenen Ebenen sinnvoll zu kombinieren und so ein dichtes Sicherheitsnetz zu knüpfen, das den Gefahren von Cyberattacken auf unterschiedliche Weise entgegentritt. Dabei haben sich vor allem folgende Sicherheitsstrategien bewährt:

Verteidigung in der Tiefe

Ausgangspunkt ist die Tatsache, dass keine Sicherheitskomponente für sich genommen einen vollständigen Schutz bieten kann. Es gibt immer ein Angriffsrisiko, sei es durch architekturbedingte Einschränkungen, Bugs oder Fehlkonfigurationen. Eine Verteidigung in der Tiefe (Defense in Depth) bedeutet, verschiedene Komponenten und Maßnahmen in mehreren Sicherheitsschichten zu kombinieren. Dazu zählen insbesondere der Einsatz von Firewalls zur Segmentierung sowie eine wirksame Zugriffskontrolle und Angriffserkennung, damit Angreifer nicht in das Netz eindringen können bzw. eine erfolgreiche Kompromittierung lokal begrenzt bleibt und frühzeitig entdeckt wird. Für



Risiken und wirkungsvolle Gegenstrategien zu ihrer Abschwächung (Mitigation) in digitalen industriellen Ökosystemen.

Industrienetze empfiehlt sich beispielsweise der Einsatz der Firewall Genuwall, die sowohl die industrielle Netzwerkkommunikation (OPC UA, Modbus TCP, IEC60870-5-104) überwacht als auch Daten auf Applikationsebene filtert. Sie unterstützt die Netzwerksegmentierung und ermöglicht ein Monitoring und Logging von Zugriffen und Änderungen.

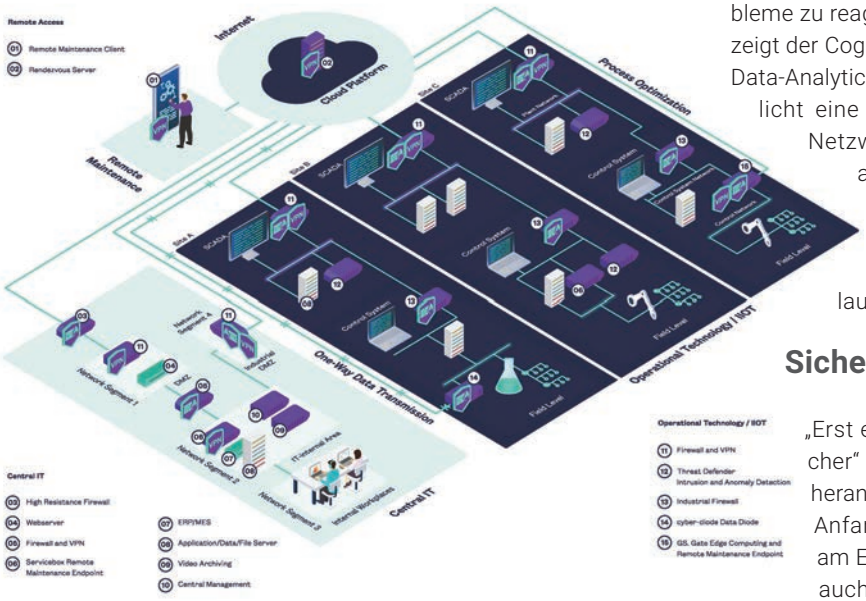
Integrierte IT/OT-Sicherheit

Durch das Öffnen der OT nach außen, zu Cloud, Office IT (z.B. ERP-Systemen) oder für externe Dienstleister, können Produktionssysteme aus Umgebungen angesprochen werden, die nicht der eigenen Kontrolle unterliegen. Diese müssen als potenziell kompromittiert bzw. böse eingestuft werden, wenn es darum geht, Kommunikation, Netz- und Dienstperimeter abzusichern. Auch hier ist der Einsatz von Firewalls auf Netz- oder Anwendungsebene unerlässlich. Generell muss die Verbindung von IT-, OT- und IIoT-Systemen mittels restriktiver, effektiver und robuster Sicherheitskonzepte abgesichert werden, um den Produktionsprozess und die Produktionsanlagen zu schützen.

Exponierte Punkte absichern

Häufig sollen in Brownfield-Projekten Fernsteuerung und -wartung ermöglicht werden. Solche Zugriffe von extern müssen restriktiv gehandhabt und überwacht werden können. Einen sicheren Betrieb ermöglicht die Fernwartungslösung Genubox, die einen Fernzugriff zulässt, diesen durch verschlüsselte Kommunikationskanäle absichert und nur eine restriktive Kommunikation beschränkt auf die zu wartenden Systeme bzw. Dienste erlaubt. Neben einer starken Authentisierung des externen Dienstleisters muss die Verbindungsaufnahme von außen immer durch innen bestätigt werden, so dass ein unberechtigter Zugriff ausgeschlossen ist. Genubox ist sowohl für externe

Dienstleister als auch für den Einsatz auf dem Shopfloor geeignet; für Industrie-Umgebungen ist sie in einer Version mit robustem Temperaturbereich und Komfortfunktionen wie z.B. einem Schlüsselschalter erhältlich. Besondere Anwendungen mit höchster Schutzklasse stellen Industrieanlagen im Bereich kritischer Infrastrukturen dar. Auch hier wird für eine effiziente Überwachung und Steuerung oftmals ein (Fern-)Zugriff auf die Daten des laufenden Betriebs benötigt. Abhilfe schaffen Daten-



Referenzarchitektur für integrierte IT/OT-Sicherheit in einer vernetzten Brownfield-Fabrik. Implementiert sind hier u.a. sichere Fernwartung, Prozessoptimierung auf Basis von Edge Computing sowie die hochsichere Datenausleitung mittels Datendiode.

dioden. Sie stellen eine besonders sichere und performante Lösung dar, bei der Daten nur in eine Richtung fließen können. Eine Fehl- oder Umkonfiguration ist ebenso ausgeschlossen wie das Öffnen einer Backdoor – die One-Way-Funktion ist nicht veränderbar. Die einzige Rückinformation ist ein Bit für die Bestätigung des erfolgreichen Datentransports.

Zero Trust Networking

Ein besonderes Augenmerk verdient das Zero-Trust-Konzept im Umfeld von digitalen Ökosystemen. Dieses geht davon aus, dass zunächst keinem Nutzer, Endgerät, Netz oder Dienst vertraut werden kann. Deshalb muss jeder Zugriff individuell verifiziert werden. Angesichts der wachsenden Komplexität, bei der die Übergänge zwischen den Netzen sowie zwischen innen und außen fließend sind, ist dies eine notwendige und angemessene Strategie. Denn potenziell ist sogar das eigene Netz unsicher – ein erfolgreicher Angriff lässt sich schließlich nicht vollkommen ausschließen. Dementsprechend müssen Firewalls, VPNs und Remote-Services so konfiguriert werden, dass eine Verbindungsaufnahme nur für festgelegte Nutzer, Applikationen und Dienste möglich ist. Darüber hinaus muss sichergestellt sein, dass sich diese jeweils zuverlässig ausweisen, bevor der Zugriff gewährt wird.

ML-basierte Netzwerksicherheit

Die beschriebenen statischen präventiven Maßnahmen können den Angreifern zwar das Eindringen erschweren, dieses aber nicht völlig ausschließen. Als ein weiteres Element im Zuge der Defense-in-Depth-Strategie sind daher reaktive Maßnahmen zur Angriffserkennung nötig. Moderne Methoden des Machine Learnings unterstützen dabei, das Netzverhalten zu verstehen, Anomalien zu detektieren und so frühzeitig auf Probleme zu reagieren. Wie dies in der Praxis funktionieren kann, zeigt der Cognitix Threat Defender von Genua mit seinen ML-, Data-Analytics- und Threat-Intelligence-Funktionen. Er ermöglicht eine dynamische Mikrosegmentierung physischer Netzwerke sowohl auf Basis statischer Regeln als auch einer dynamischen Verhaltensanalyse in Echtzeit. Bei anomalem Verhalten einer Netzwerkressource oder eines Nutzers können automatisch die Zugangsrechte entzogen und so laufende Angriffe in Echtzeit gestoppt werden.

Sicherheit von Anfang an

„Erst einmal muss es laufen, dann machen wir es sicher" – wer heute noch auf diese Weise an ein Projekt herangeht, muss zwangsläufig scheitern. Nur wer von Anfang an Security mitdenkt, kann sicher sein, dass am Ende eine Lösung steht, die sowohl funktional als auch sicher ist. Dementsprechend sollten die vorgenannten Tipps bereits bei der Konzeption von Netzwerken beachtet werden. Aber auch die Entwicklung von Geräten und Services muss diesem Gedanken folgen. Im industriellen Umfeld gilt sogar noch eine weitere Bedingung: Nicht nur Security, sondern auch Robustness by Design sollte das oberste Entwicklergebot lauten. Wo es nicht möglich ist, dieses Prinzip bei den OT-Komponenten durchzusetzen – etwa bei bestehenden Installationen – muss es zumindest bei den eingesetzten Sicherheitssystemen gelten. Erreicht werden kann dies über ein In-Depth-Softwaredesign, das über etablierte Konzepte wie Privilege Separation oder Sandboxing die Angriffsfläche verringert und so eine robuste Sicherheit gewährleistet. Flankiert werden sollte die Entwicklungsarbeit durch externe Evaluationen und Zertifizierungen, um aus unabhängiger Sicht Design und Umsetzung zu überprüfen. Genua stellt sich diesen Anforderungen und kann entsprechende Zertifizierungen und Zulassungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorweisen. Dieses hat u.a. die Firewall Genugate des Sicherheits-Experten nach Common Criteria EAL4+ (CC EAL4+) zertifiziert. Auch das von Genua entwickelte Patch-Management (ALC_PAM), das einen effektiven Schutz von Softwareupdates gegen Infiltrationsversuche bietet, ist Teil der Zertifizierung. So können Anwender sicher sein, dass die Systeme nicht über gefälschte Updates angreifbar sind. ■

Direkt zur Übersicht auf
i-need.de
www.i-need.de/f/4370

Harry Jacob,
freier Journalist
Genua GmbH
www.genua.de/digitale-industrie

Bild: genua gmbH